

TO: Clerk's Office
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK



APPLICATION FOR LEAVE
TO FILE DOCUMENT UNDER SEAL

IN THE MATTER OF SEARCH OF
 PREMISES KNOWN AS [REDACTED]
 [REDACTED] BROOKLYN, NEW YORK 11234,
 AND ANY AND ALL COMPUTERS,
 CELLULAR TELEPHONES AND ELECTRO

24-MC-2339
 Docket Number

SUBMITTED BY: Plaintiff___ Defendant___ DOJ ☒
 Name: Leonid Sandlar
 Firm Name: U.S. DOJ; USAO-EDNY
 Address: 271-A Cadman Plaza East
 Brooklyn, NY 11201
 Phone Number: 718-254-5879
 E-Mail Address: leonid.sandlar@usdoj.gov

INDICATE UPON THE PUBLIC DOCKET SHEET: YES___ NO ☒
 If yes, state description of document to be entered on docket sheet:

MANDATORY CERTIFICATION OF SERVICE:

A.) ___ A copy of this application either has been or will be promptly served upon all parties to this action, B.) ___ Service is excused by 31 U.S.C. 3730(b), or by the following other statute or regulation: ___; or C.) ☒ This is a criminal document submitted, and flight public safety, or security are significant concerns. (Check one)

06/12/2024
 DATE

Leonid Sandlar
 SIGNATURE

A) If pursuant to a prior Court Order:

Docket Number of Case in Which Entered: _____
 Judge/Magistrate Judge: _____
 Date Entered: _____

B) If a new application, the statute, regulation, or other legal basis that authorizes filing under seal

Ongoing criminal investigation _____

**ORDERED SEALED AND PLACED IN THE CLERK'S OFFICE,
 AND MAY NOT BE UNSEALED UNLESS ORDERED BY
 THE COURT.**

DATED: Brooklyn, NEW YORK
 June 12, 2024

U.S. MAGISTRATE JUDGE

RECEIVED IN CLERK'S OFFICE _____
 DATE

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF SEARCH OF
PREMISES KNOWN AS [REDACTED]
[REDACTED] BROOKLYN, NEW YORK 11234,
AND ANY AND ALL COMPUTERS,
CELLULAR TELEPHONES AND
ELECTRONIC DEVICES CONTAINED
THEREIN

TO BE FILED UNDER SEAL

**APPLICATION FOR A
SEARCH WARRANT FOR A PREMISES
AND ELECTRONIC DEVICES FOUND
THEREIN**

Case No. 24-MC-2339

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A WARRANT TO
SEARCH AND SEIZE**

I, [REDACTED] being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

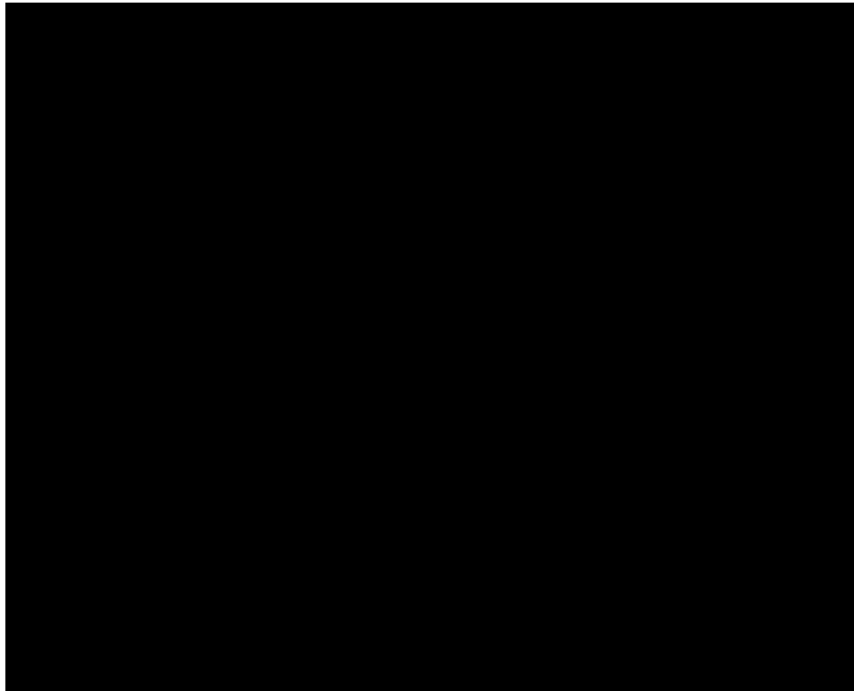
1. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises specified below and in Attachment A (the "SUBJECT PREMISES"), namely [REDACTED] Brooklyn, NY [REDACTED] and to seize, the items and information described in Attachment B.

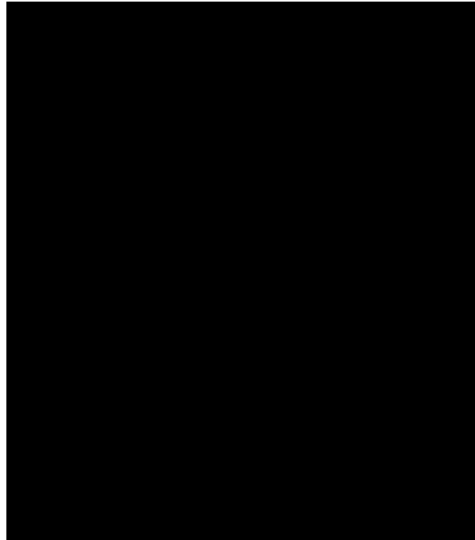
2. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since 2019. I am currently assigned to a public corruption squad of the New York Field Office, where, among other things, I investigate crimes involving illegal campaign contributions, theft of federal funds, and bribery. Through my training and experience, I also have become familiar with some of the ways in which individuals use smart phones and electronic communications, including social media, email, and electronic messages, in furtherance of their crimes, and have participated in the execution of search warrants involving electronic evidence.

3. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

IDENTIFICATION OF THE SUBJECT PREMISES

4. The SUBJECT PREMISES is a detached single-family home located at [REDACTED] Brooklyn, New York 11234. The SUBJECT PREMISES is accessed by a door up a short flight of stairs from the driveway and sidewalk, with the number [REDACTED] inscribed on an archway approaching the doors. A photograph of the SUBJECT PREMISES, as well as and a close-up of the archway before the door, is included below.





THE SUBJECT OFFENSES

5. For the reasons detailed below, I respectfully submit that there is probable cause to believe that the SUBJECT PREMISES contains evidence, fruits, and instrumentalities of violations of (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds and conspiracy to steal federal funds, federal program bribery, and conspiracy to commit the same); (ii) 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt and conspiracy to commit wire fraud); (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same); and (iv) 18 U.S.C. § 1956 (money laundering and conspiracy to commit money laundering) (collectively, the “SUBJECT OFFENSES”), committed by [REDACTED] among others.

PROBABLE CAUSE

A. Probable Cause Regarding the Subjects’ Commission of the Subject Offenses

6. Since in or about August 2021, the FBI and the Office of the United States Attorney for the Southern District of New York have been investigating the receipt of so-called “straw” donations by the 2021 and 2025 New York City mayoral campaigns of Eric Adams (the “2021 Adams Campaign,” the “2025 Adams Campaign,” and, collectively, the “Adams Campaigns”),

including certain straw donations that were funded by and/or made at the direction of foreign government officials and other foreign persons.¹

7. As part of this investigation, law enforcement has obtained various warrants for electronic evidence, including:

a. On or about April 5, 2024, the Hon. Robyn F. Tarnofsky, United States Magistrate Judge for the Southern District of New York, signed a warrant authorizing the search of an iCloud account used by [REDACTED] (the “[REDACTED] iCloud Warrant”). A copy of the [REDACTED] iCloud Warrant is attached as Exhibit 1 to this Affidavit.

b. On or about June 6, 2024, the Hon. Stewart D. Aaron, United States Magistrate Judge for the Southern District of New York, signed a warrant and order directing Verizon Wireless to provide prospective cellphone location information and historical cellphone location information back to May 15, 2024, among other information, for a cellphone subscribed to [REDACTED] (the “[REDACTED] Cellphone” and, for the warrant, the “[REDACTED] Cellphone Warrant”). A copy of the [REDACTED] Cellphone Warrant is attached as Exhibit 2 to this Affidavit.

8. This application seeks a warrant to search a premises, the SUBJECT PREMISES, including electronic devices found therein, used by [REDACTED]. As discussed below, the investigation has developed evidence that [REDACTED] is connected to the Government of Uzbekistan and works to influence Adams on behalf of Uzbek and Central Asian causes. [REDACTED] has also coordinated straw donations to the Adams Campaigns and sought Adams’s assistance in connection with New York City business on at least one occasion regarding

¹ A straw, or “conduit,” donation occurs when a donation to a political campaign is made in the name of one donor, but the funds in question in fact belong to a different person.

██████████'s real estate business. ██████████ further appears to have engaged in money laundering to support that business.

The Adams Campaign and New York City's Matching Funds Program

9. I understand, based on my review of publicly available information, that:

a. The Adams Campaigns accepted Matching Funds from the New York City Campaign Finance Board throughout a significant part of its campaign, meaning that the Adams Campaigns received funds from the New York City government as a result of donations the Adams Campaigns received from private donors that were eligible for matching funds.²

b. Under New York City law, the Adams Campaigns were eligible to receive \$2,000 in matching funds, and no more than \$2,000 in Matching Funds, for each donation of \$250 from an individual donor who resides within New York City, subject to certain exceptions not relevant here. If an individual donated more than \$250, any amount in excess of \$250 would not be eligible for matching funds.³

c. New York City receives in excess of \$10,000 per year in federal funding.⁴

Adams Receives Straw Donations and Travel Benefits

10. Based on my review of records from the New York City Campaign Finance Board, I know that on or about May 7, 2021, the 2021 Adams Campaign received approximately eleven

² See, e.g., <https://ny1.com/nyc/all-boroughs/news/2021/10/08/eric-adams-is-taking-a-rare-step--turning-down-campaign-cash> (reporting on the Adams Campaign's prior acceptance of matching funds and decision to turn down some matching funds as of October 7, 2021); https://www.nyccfb.info/VSApps/CandidateSummary.aspx?as_cand_id=1545&as_election_cycle=2021&cand_name=Adams%2C+Eric+L&office=Mayor&report=summ (New York City Campaign Finance Board's report detailing total public funds disbursed to 2021 Adams Campaign).

³ See <https://www.nyccfb.info/candidate-services/join/>.

⁴ See, e.g., https://comptroller.nyc.gov/wp-content/uploads/2016/11/Federal_Budget_Vulnerabilities_Memo.pdf.

donations from employees of [REDACTED] in amounts that ranged from approximately \$1,200 to \$1,500.⁵ On or about April 28, 2021, [REDACTED] issued checks to the same individuals, with one exception, for approximately \$1,250.⁶

11. Based on my review of email messages with [REDACTED] Turkey's Consul General in New York, I know that [REDACTED] was involved in arranging the fundraiser at which the [REDACTED] donations were made. For instance, on or about April 21, 2021, an owner of [REDACTED] Construction sent an email to four individuals stating, in substance and in part, that he had spoken with "Consul General Mr. [REDACTED] who was very happy and thought that mid-May would be an appropriate target date.

12. Based on my review of Adams's financial records and travel records, among other evidence, I have learned that Adams and others associated with him traveled to Turkey on [REDACTED] on trips that were provided at no cost or at reduced cost.

[REDACTED] *is Connected to Both the Government of Uzbekistan and Adams*

13. [REDACTED] is the founder of the Silk Road Foundation, an organization that purports to support families that have migrated to the United States from Central Asia.⁷ Based on my review of records from a law enforcement database, I know that [REDACTED] is a dual American and Uzbek citizen.

⁵ Certain earlier affidavits in this investigation stated that [REDACTED] was affiliated with a larger Turkish corporation. Law enforcement has since interviewed several [REDACTED] employees who have stated, in substance and in part, that although [REDACTED] was started by personnel formerly employed by that larger Turkish corporation, the two entities have no formal connection.

⁶ One check was issued to someone whom I know from law enforcement databases is the spouse of a donor.

⁷ See <https://www.brooklynbp.nyc.gov/nearly-200-brooklynites-join-brooklyn-borough-president-antonio-reynoso-for-second-annual-ramadan-iftar-at-borough-hall/>.

14. [REDACTED]'s social media indicates that he works with the Government of Uzbekistan to promote Uzbek causes in the United States. For instance, in substance and in part:

a. In or about the summer of 2023, [REDACTED] posted a picture on social media with a caption that he was at a "dinner with Uzbek officials" where "we discussed the rich heritage of Uzbekistan and how we can together help promote it in the United States."

b. Also in or about the summer of 2023, [REDACTED] posted a picture with a caption stating: "We met with the Minister of Natural Resources of Uzbekistan, Mr. [REDACTED] today"

c. In or about late 2023, [REDACTED] posted a picture of a watch in a ceremonial case. The caption says, "Thank you Mr. President" and tags the account of the President of Uzbekistan.

15. Based on my review of records from a phone company for the [REDACTED] Cellphone, I have learned that the phone is subscribed to [REDACTED] and that between on or about April 9, 2023, and on or about January 17, 2024, the [REDACTED] Cellphone had approximately 292 communications with a phone with a number ending in 0440. Based on my review of records from a law enforcement database, I know that the 0440 number is used by a member of the Uzbekistan Permanent Mission to the United Nations.

16. Based on my review of social media posts, I have also learned that [REDACTED] attends official events with Adams. For instance, in substance and in part:

a. In or about April 2023, [REDACTED] posted two photos on social media. One is captioned: "Attended a fantastic iftar event hosted by Mayor Eric Adams yesterday! It was incredible!" The other is a photo of [REDACTED] with Adams, captioned "With the Mayor of NYC Eric L. Adams #nycmayor."

b. On or about July 18, 2023, an organization named “Makonim USA” posted on Facebook describing a “HISTORIC EVENT”: “the 1st ever Uzbek community roundtable with Mayor Eric Adams took place inside City Hall. . . . Very proud of Silk Road Foundation and [REDACTED] [REDACTED] for being the leaders who really care about their community and working hard to bring resources to their people.”

c. Also in approximately July 2023, [REDACTED] posted a photo of himself with Adams. The photo was captioned “Dear Gosht team, congratulations on the grand opening! Wishing you success, growth, and prosperity!!!” The post also stated that it was located in Brooklyn, New York. According to open-source information, there is a halal restaurant named Gosht in Brooklyn.

d. In or about September 2023, [REDACTED] posted a photo of himself with Adams. The photo was captioned “Happy Uzbekistan Independence Day! . . . Mayor Eric Adams made history by being the first to raise the Uzbek flag on Wall Street! A proud moment for NYC’s vibrant Uzbek community.” Based on my review of public posts for an account on X.com (formerly Twitter.com) belonging to Adams, I know that Adams also posted pictures from a flag raising on Uzbekistan Independence Day.”⁸

17. Based on my review of phone records for the [REDACTED] Cellphone, I have learned the following:

a. In or about 2023, [REDACTED] had approximately one call with a phone number ending in 3179. Based on my participation in the investigation, including my review of electronic devices belonging to Adams, I believe that the 3179 number is the number of Adams’ personal cellphone.

⁸ See <https://twitter.com/NYCMayor/status/1698035304978927860>.

b. In or about October 2023, [REDACTED] had approximately two calls with a phone number ending in 2780. Based on my participation in the investigation, including my review of electronic devices belonging to [REDACTED]—a fundraiser for the Adams Campaigns—the 2780 number is used by [REDACTED]

18. Between in or about January 2023 and in or about January 2024, [REDACTED] had approximately fifty-five calls with a phone number ending in 0470. Based on my review of records from a law enforcement database, I have learned that the 0470 number is used by [REDACTED] the Commissioner for the New York City Office of Community Affairs.

[REDACTED] Coordinates Straw Donations to the Adams Campaigns

19. I know from my review of review of records from the New York Campaign Finance Board that on or about December 10, 2020, [REDACTED] and four other individuals donated by check approximately \$2,000 each to the 2021 Adams Campaign. Based on my review of the donors' contribution cards, I have learned the following, in substance and in part:

a. Four of the donors—all except [REDACTED]—list their employer as [REDACTED]. [REDACTED] lists his employer as "Self," with his occupation as "President," lists an email address with a [REDACTED].com domain name, and lists the same employer address as the other individuals. I therefore believe that [REDACTED] was the President of [REDACTED] and the other four donors worked for him. This pattern of donations is materially similar to the [REDACTED] donations discussed above, which I have confirmed, through admissions of the donors and other evidence, were straw donations.

b. All five of the contribution cards have matching, pre-typed information, including the recipient and the names and addresses of the respective donors and their employers. Based on

my experience reviewing contribution cards, I have observed that contribution cards are often filled in by hand, and the use of pre-typed cards is unusual.

c. Because the donations were made on the same day in matching amounts by employees of the same organization using substantially similar contribution cards, I believe they were coordinated.

20. Based on my review of the bank records of the five donors, I believe that at least one donor was reimbursed for the donation. Specifically, one of the donors described in Paragraph 19 is [REDACTED] who is listed on his contribution card as a Project Manager for [REDACTED]

[REDACTED] Based on my review of [REDACTED] bank records, a check from [REDACTED] account to the 2021 Adams Campaign for approximately \$2,000 is dated on or about December 10, 2020, and cleared on or about December 22, 2020. Also on or December 10 and 21, 2020 [REDACTED] account received two cash deposits totaling approximately \$2,000. Accordingly, [REDACTED] received approximately \$2,000 in cash at approximately the same time he gave approximately \$2,000 to the 2021 Adams Campaign.

21. Based on my review of [REDACTED]'s bank records, I have learned that in or about December 2020—around the time [REDACTED] donated \$2,000 to the 2021 Adams Campaign—[REDACTED] received a number of deposits to the same bank account in the approximate amount of \$2,000 to \$3,000. While I am not at this time able to identify any specific deposit as a reimbursement for [REDACTED]'s donation, and such a reimbursement may not have occurred, these deposits are also consistent with such a reimbursement.

22. Based on my review of the bank records of the other three donors, I have learned that one appears to have deposited approximately \$2,000 in cash in two payments (as well as an additional deposit of approximately \$1,300) at approximately the same time as the \$2,000

donation; one made a deposit of approximately \$1,200 at approximately the same time as the \$2,000 donation; and one does not appear to have made a deposit at approximately that time.

23. I also know from my review of records from the New York Campaign Finance Board that on or about June 13 and 14, 2023, [REDACTED] and six other individuals, among others, donated to the 2025 Adams Campaign as follows:

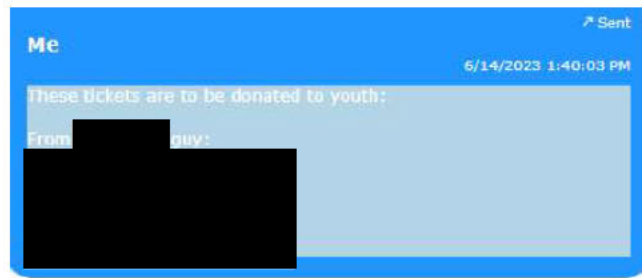
Name	Amount
[REDACTED]	\$1,000
[REDACTED]	\$1,000
[REDACTED]	\$1,000
[REDACTED]	\$1,000
[REDACTED]	\$1,000
[REDACTED]	\$1,000
[REDACTED]	\$1,000

24. Public reporting states that the 2025 Adams Campaign hosted a fundraiser on Broadway on or about June 16, 2023.⁹

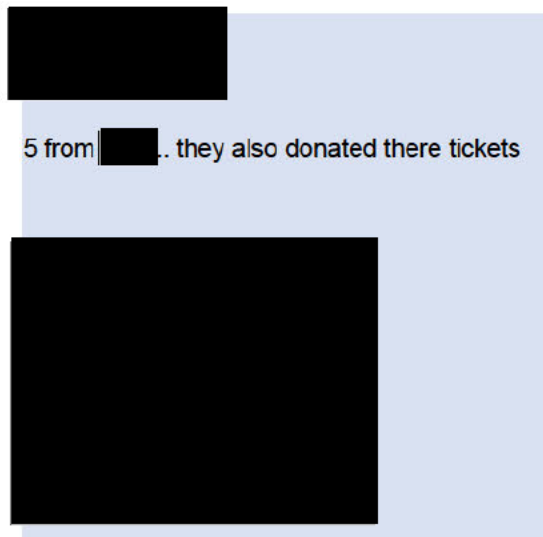
25. Based on my review of messages obtained from electronic devices belonging to [REDACTED] pursuant to a search warrant, I have learned the following:

a. On or about June 14, 2023, [REDACTED] sent the following message:

⁹ See <https://www.cityandstateny.com/politics/2023/06/eric-adams-fundraising-broadway-show-new-york-new-york/387039/>.



b. On or about June 16, 2023, [REDACTED] received a message from a phone number identified as [REDACTED] is likely [REDACTED] who I know from my participation in this investigation is a senior advisor to Adams for South Asian and Muslim Affairs. The message to [REDACTED] states:



The seven names in this message are the same seven names identified as donors to the 2025 Adams Campaign in Paragraph 23.

c. Based on the above messages, I believe that [REDACTED] coordinated five of the donations, including his own donation, and that all of the donors donated their tickets rather than attend the Broadway fundraiser.

26. Review of records obtained pursuant to the [REDACTED] iCloud Warrant remain ongoing. However, among other messages, I have identified the following:

a. The phone contains an SMS message thread between [REDACTED] and a contact named “Mayor Adams,” using the 3179 number discussed above.

b. On or about June 13, 2023, Adams messaged [REDACTED] a donation link for his campaign and asked [REDACTED], in part, to “ask friends and family to contribute.” Adams also asked [REDACTED] to “please forward the names” of donors “for our record.”

c. The next day, [REDACTED] and Adams exchanged a series of messages. In substance and in part, they stated the following:

i. [REDACTED] sent Adams the same five names, including his own, discussed in the prior paragraph. [REDACTED] also stated, “Tomorrow will do more.”

ii. Adams asked whether they had already donated, and [REDACTED] confirmed, stating that “I have all receipts.”

iii. Adams asked whether they were attending the fundraiser or “donating to homeless youth,” which I believe means donating their tickets to the fundraiser. [REDACTED] responded that “We” would donate the tickets. [REDACTED] added that Adams “can text me on Signal also,” which Adams acknowledged. Based on my experience and participation in this and other investigations, I know that Signal is an encrypted messaging application. Signal messages often do not back up to iCloud accounts and cannot be obtained by an iCloud search warrant, and no Signal messages were recovered pursuant to the [REDACTED] iCloud Warrant.¹⁰

¹⁰ Signal messages can be recovered by a search of a physical cellphone or other electronic device, although the availability of messages may depend on whether the user has set the application to autodelete messages at certain intervals. In the course of this investigation, I have learned that on at least some occasions, Signal threads with Adams were set to autodelete, and I have obtained Signal messages from physical devices that were not found on the iCloud accounts of the devices’ user.

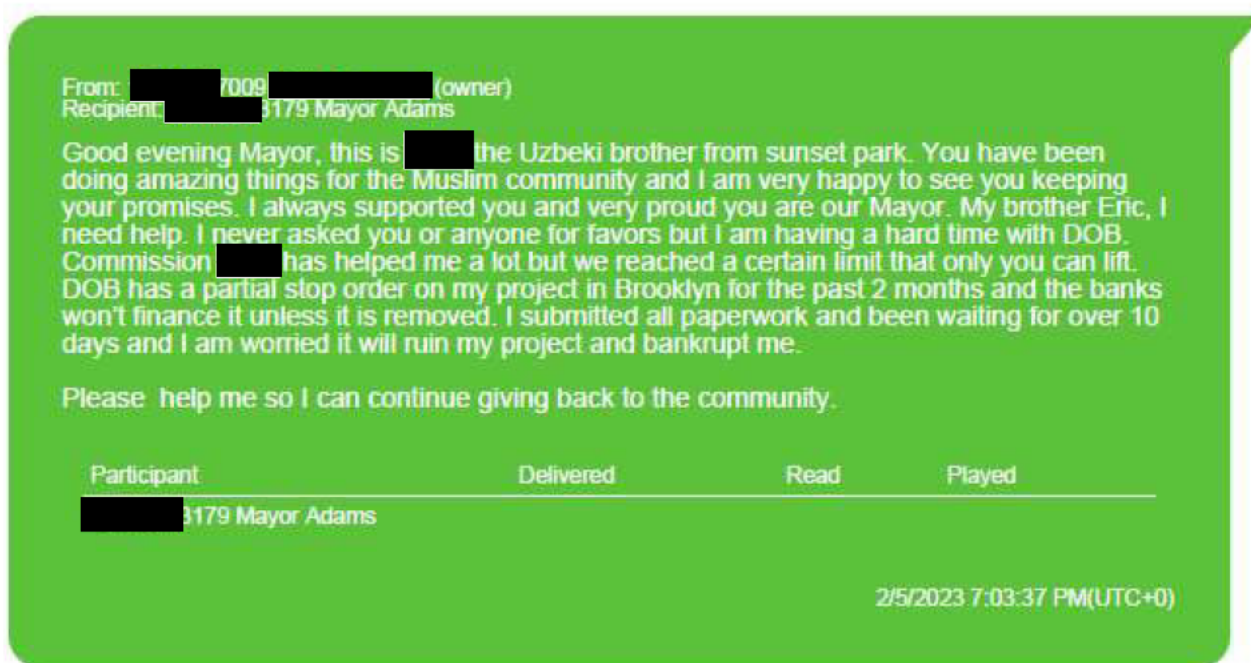
27. Based on my review of bank records for the five donors discussed in the previous paragraph, I have identified what appears to be a reimbursement payment for one of the donors. Specifically, on or about June 20, 2023, approximately one week after the donations described in Paragraph 23 above, [REDACTED] sent [REDACTED] via Zelle approximately \$1,000—the same amount as [REDACTED] donation to the 2025 Adams Campaign. I have not identified reimbursement payments for the remaining donors.

28. Based on my review of materials obtained from [REDACTED] electronic devices pursuant to a search warrant, I have learned that on or about October 10, 2023, [REDACTED] sent a message to the [REDACTED] Cellphone stating, in substance and in part, “This is [REDACTED] Mayor Adams’ fundraiser. I’m reaching out regarding scheduling a fundraiser, can you please give me a call back when you have a moment?” That phone number appears in [REDACTED] Apple Contacts as the number for [REDACTED] and the organization is listed as “Uzbek/ Brooklyn.”

[REDACTED] *Received Assistance from Adams*

29. Based on my review of the SMS message thread between [REDACTED] and Adams discussed above, I have learned the following:

a. On or about February 5, 2023, [REDACTED] sent Adams the following message, in substance and in part, at the 3179 number discussed above:



b. Based on my review of other messages obtained pursuant to the [REDACTED] iCloud Warrant, I believe that in the above-referenced message [REDACTED] refers to the fact that the New York City Department of Buildings (“DOB”) had issued a partial stop work order on one of [REDACTED]’s real estate projects.

c. Later that evening, Adams responded, in sum and substance, “Let me look into this.”

d. On or about February 14, 2023, [REDACTED] messaged Adams again stating, in substance and in part, “thank you for your help,” and the “DOB issue” was “partially resolved.” [REDACTED] added that Adams has “my continued support.”

Adams Explores Travel to Uzbekistan

30. Based on my review of the SMS message thread between [REDACTED] and Adams discussed above, I have learned the following in substance and in part:

a. On or about June 16, 2023, [REDACTED] messaged Adams stating that, in substance and in part, [REDACTED] “received the information that you are planning to visit Uzbekistan on July 7-9th. Just wanted to confirm with you that this is 100%.”

b. Adams responded, in sum and substance, that “We are looking into it.”

c. [REDACTED] replied, in substance and in part, “Please let me know if you need anything. . . . This is amazing news, me and the Ambassador are excited for this historic trip and waiting for confirmation from your team so we can start the coordination. Please let me know if anything is needed from my end.”

d. This investigation has not uncovered evidence that Adams in fact travelled to Uzbekistan. As noted above, however, Adams accepted free or discounted travel from the Turkish consulate.

[REDACTED] Appears to Have Separately Engaged in Money Laundering Activity

31. Based on my review of bank records, I have learned the following:

a. Along with another individual (“Individual-1”), who also donated to the 2021 Adams Campaign as an employee of [REDACTED], as discussed above, [REDACTED] is a signatory for a bank account in the name of [REDACTED]

b. On or about January 24, 2020, [REDACTED] received a wire in the amount of approximately \$11.7 million from [REDACTED] a Cyprus-based entity.

c. Approximately three days later [REDACTED] wired approximately \$11.7 million to another bank account, also in the name of [REDACTED], and also for which [REDACTED] and Individual-1 were signatories.

d. Approximately three days later, [REDACTED] wired approximately \$11.7 million in two transfers to two bank accounts. Approximately \$11.5 million were transferred to

an account in the name of [REDACTED] ending in 3167 (the “3167 [REDACTED] Account”), and for which [REDACTED] and Individual-1 were signatories. The remaining approximately \$200,000 were transferred to another account in the name of [REDACTED], this one ending in 8865 (the “8865 [REDACTED] Account”), and for which [REDACTED] and Individual-1 were signatories.

e. Approximately one week later, on February 6, 2020, [REDACTED] wired approximately \$11.5 million from the 3167 [REDACTED] Account to the 8865 [REDACTED] Account.

f. The same day, on or about February 6, 2020, the 8865 [REDACTED] wired approximately \$11.7 million to a company called [REDACTED]

g. Based on my review of New York City real estate records, I have learned that on or about February 7, 2020, [REDACTED] purchased a building in Brooklyn, New York, for approximately \$13 million.

32. Based on my participation in money laundering investigations, I know that the rapid movement of large sums of money between accounts, as described above, is indicative of an effort to conceal or disguise the nature and source of the funds.

B. Probable Cause Justifying Search of the Subject Premises

33. I know, based on my review of Apple account records and subscriber records from a telephone company, that [REDACTED] listed the SUBJECT PREMISES as his address. I also know, based on my review of data obtained pursuant to the [REDACTED] Cellphone Warrant, that [REDACTED] has spent many nights over the last several weeks at the SUBJECT PREMISES.

34. Based on my review of Apple account records and materials obtained pursuant to the [REDACTED] iCloud Warrant, I have learned that since in or about 2010, [REDACTED] has obtained multiple Apple cellphones and iPads, two computers, and an Apple Vision Pro headset.

Based on my participation in this investigation and my training and experience, I know that each of these devices is capable of storing electronic messages and/or other communications data.

35. Based on my training and experience, persons generally keep their cellphones, laptops, and tablets (such as iPads) accessible, meaning that if a person is at home, those devices are likely to be in their residence. I am aware, including based on the communications described above, that [REDACTED] used electronic communications in furtherance of the SUBJECT OFFENSES. Based on my training and experience, electronic communications, including emails and text messages, are frequently stored on persons' cellphones, laptops, and tablets. In addition, based on my training and experience and my involvement in this investigation, I know that persons often receive financial records, including bank and credit card statements that may reflect the provision or receipt of pecuniary benefits, by mail to their residence.

C. Probable Cause Justifying Search of ESI

36. For the reasons set forth above, there is probable cause to believe that cellphones, tablets (including Apple iPads), and computers used by [REDACTED] will contain evidence of the SUBJECT OFFENSES. In addition to the evidence discussed above that [REDACTED] has used such devices to communicate about the SUBJECT OFFENSES, there is probable cause to believe that cellphones, tablets (including Apple iPads), and computers used by [REDACTED] will contain evidence of the SUBJECT OFFENSES for these additional reasons:

a. Computers, tablets, and cellphones can be used store documents, including emails, text messages, previous electronic chats, and financial documents like bank statements and travel expenditure. Tablets and computers can also be used to create documents in word processing programs, like Microsoft Word. Document attachments to communications can be saved intentionally or as a result of a cellphone's or tablet's operating system or web browser to an electronic device, including a computer, tablet, or cellphone. Moreover, and more generally, users

of cellphones, tablets, and computers who are engaged in the commission of the SUBJECT OFFENSES often store documents relevant to that activity on their devices, and also maintain notes of meetings and telephone calls on their devices. Such documents can include, but are not limited to, Microsoft Word and PDF documents, drafts, scans, bank statements received from financial institutions, and government filings.

b. Cellphones, tablets, and computers can contain photographs and videos of meetings—such as the images relating to Adams and Uzbek officials discussed above—and documents, audio recordings of telephone calls and meetings, and screenshots of text messages.

c. Electronic files, or remnants of those files, downloaded to a cellphone, tablet, or computer can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person “deletes” a file on a cellphone, tablet, or computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space—for long periods of time before they are overwritten. In addition, a device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a cellphone, tablet, or

computer depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and cellphone habits.

d. Additionally, a person can transfer data from an old cellphone, tablet, or computer to a new device, including, for example, mail, contacts, calendars, photos and videos, books and pdfs, call logs, and text messages. For individuals who regularly change or upgrade their devices, including cellphones, it is common to transfer electronic records, such as emails, contacts, calendars, photos and videos, books and pdfs, call logs, and text messages from the old phone to a new phone. Individuals can transfer data in a few ways, including in a cellphone provider or Apple store, through a personal computer containing a backup, or through an iCloud backup. Accordingly, data found on one electronic device is often found on other devices used by the same person.

e. As discussed above, [REDACTED] is known to use encrypted messaging applications, including Signal, to send messages. Such messages can sometimes be recovered from physical electronic devices even where they cannot be recovered from an iCloud backup.

f. Accordingly, there is probable cause to believe that evidence, fruits, and instrumentalities of the SUBJECT OFFENSES listed in Attachment B, which is incorporated by reference herein, will be found in the SUBJECT PREMISES, and on electronic devices found in the SUBJECT PREMISES.

37. Based on the foregoing, I respectfully submit there is probable cause to believe that [REDACTED] has committed the SUBJECT OFFENSES, and that evidence of this criminal activity is likely to be found in the SUBJECT PREMISES and on computers and electronic media found in the SUBJECT PREMISES.

PROCEDURES FOR SEARCHING ESI

38. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review.” Consistent with Rule 41, this application requests authorization to seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.
- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.
- Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.
- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

AUTHORITY TO OBTAIN BIOMETRIC DATA

39. I know from my training and experience, as well as from information found in publicly available materials, that Apple iPhones and iPads offer their users the ability to unlock the device via biometric features (e.g., fingerprint, facial recognition) in lieu of a numeric or alphanumeric passcode or password. Apple’s fingerprint recognition feature is called Touch ID, and its facial recognition feature is called Face ID.

40. If a user enables Touch ID on a given device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device.

41. If a user enables Face ID on a given device, he or she can unlock the device by raising the iPhone to his or her face.

42. In my training and experience, users of devices that offer Touch ID or Face ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents.

43. In some circumstances, Touch ID or Face ID cannot be used to unlock a device that has either security feature enabled, and a passcode or password must be used instead. These circumstances include: (1) when the device has just been turned on or restarted; (2) when more than 48 hours has passed since the last time the device was unlocked; (3) when the passcode or password has not been entered in the last 6 days, and the device has not been unlocked via Touch ID in the last 8 hours or the device has not been unlocked via Face ID in the last 4 hours; (4) the device has received a remote lock command; or (5) five unsuccessful attempts to unlock the device via Touch ID or Face ID are made.

44. The passcodes or passwords that would unlock electronic devices subject to seizure pursuant to the requested warrant are unknown to law enforcement. Thus, it will likely be necessary to press [REDACTED]'s fingers to any Touch ID sensors, or to hold those devices in front of [REDACTED]'s face to activate the Face ID sensor, in an attempt to unlock those devices

for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant devices via Touch ID with the use of the fingerprint of the user, or via Face ID by holding the device in front of the user's face, is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

45. Although I do not know which of a given user's 10 fingerprints are capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock any electronic devices as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

46. I also know from my training and experience, and my review of publicly available materials that Apple brand devices have a feature that allows a user to erase the contents of the device remotely. By logging into the Internet, the user or any other individual who possesses the user's account information can take steps to completely wipe the contents of the device, thereby destroying evidence of criminal conduct, along with any other information on the device. The only means to prevent this action is to disable the device's ability to connect to the Internet immediately upon seizure, which requires either access to the device itself to alter the settings, or the use of specialized equipment that is not consistently available to law enforcement agents.

47. Due to the foregoing, I request that the Court authorize law enforcement to press [REDACTED]'s fingers (including thumbs) to the Touch ID of any seized devices, or to hold those devices in front of [REDACTED]'s face (and, if necessary, to hold [REDACTED] in place while

holding the electronic devices in front of his face), for the purpose of attempting to unlock the devices via Touch ID or Face ID in order to search the contents as authorized by this warrant.

REVIEW OF ESI

48. Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

49. The full scope of this ongoing criminal investigation is not publicly known. Although the execution of the requested warrant will reveal to [REDACTED] the general existence of an investigation into the SUBJECT OFFENSES, it will not reveal its full scope, including the witnesses and evidence discussed in this affidavit. Premature public disclosure of this affidavit could cause [REDACTED] and his associates and co-conspirators to destroy evidence not yet gathered by law enforcement, much of which likely exists in electronic or paper forms that can be readily destroyed. In addition, disclosure of this affidavit could cause the subjects of this investigation to believe that their arrest is imminent, triggering their flight. That is especially concerning given that some of the subjects of the investigation discussed herein have significant ties abroad (as partly discussed in this Affidavit). For these reasons, I respectfully request that this Affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as needed to personnel assisting in the investigation and

prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

CONCLUSION

50. Based on the foregoing, I respectfully request the court to issue a warrant to search the SUBJECT PREMISES described in Attachment A, and to seize the items and information specified in Attachment B to this Affidavit and to the Search and Seizure Warrant.

Respectfully submitted,



Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me by telephone on June 12, 2024

A handwritten signature in cursive script, appearing to read 'Peggy Kuo', written over a horizontal line.

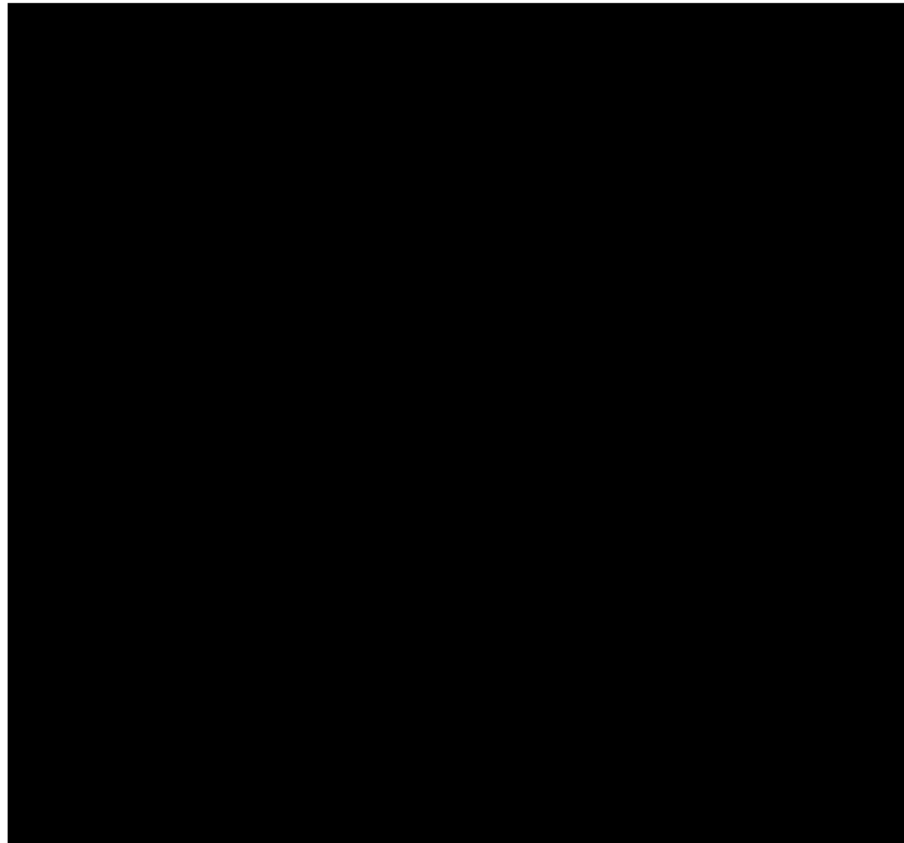
HON. PEGGY KUO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

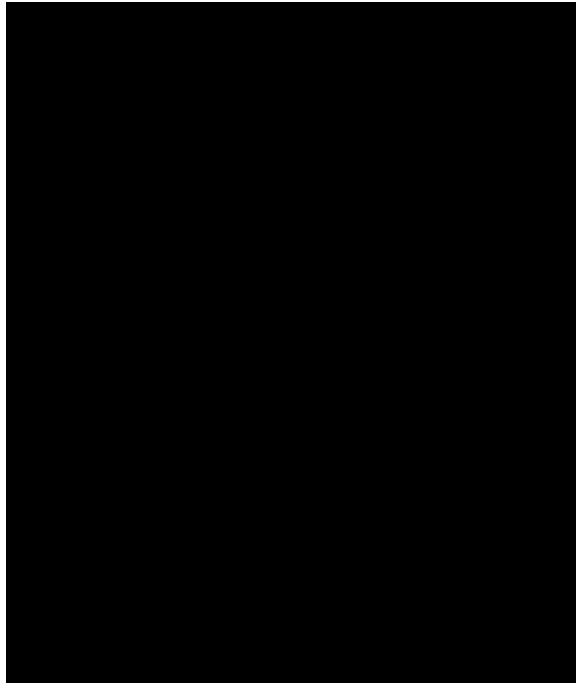
ATTACHMENT A

Premises to be Searched—Subject Premises

The premises to be searched (the “SUBJECT PREMISES”) are described as follows, and include all locked and closed containers found therein:

The SUBJECT PREMISES is a detached single-family home located at [REDACTED] [REDACTED] Brooklyn, New York 11234. The SUBJECT PREMISES is accessed by a door up a short flight of stairs from the driveway and sidewalk, with the number [REDACTED] inscribed on an archway approaching the doors. A photograph of the SUBJECT PREMISES, as well as and a close-up of the archway before the door, is included below.





ATTACHMENT B

Items to Be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the SUBJECT PREMISES consist of the following evidence, fruits, and instrumentalities of violations (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds and conspiracy to steal federal funds, federal program bribery, and conspiracy to commit the same), (ii) 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt and conspiracy to commit wire fraud), (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same), and (iv) 18 U.S.C. § 1956 (money laundering and conspiracy to commit money laundering) (collectively, the “SUBJECT OFFENSES”), described as follows:

1. Evidence concerning occupancy or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.

2. Electronic devices, including cellphones, laptops, and tablets, owned or used by [REDACTED] (hereinafter, the “Seized Devices”).

3. Evidence regarding the identity of the owner or user of the Seized Devices at times relevant to the Subject Offenses.

The Seized Devices may be searched for the following evidence, fruits, and instrumentalities of the Subject Offenses:

A. Evidence of knowledge or understanding of, or intent to violate, laws and regulations governing the conduct of the Adams Campaigns on the part of [REDACTED] and his employees or associates, or the Adams Campaigns.

B. Evidence relating to coordination between [REDACTED] and the Adams Campaigns concerning political contributions to the Adams Campaigns, including, but not limited to, evidence of motive and intent for [REDACTED] or his employees or associates to provide or facilitate campaign contributions to the Adams Campaigns, and evidence of motive and intent by any person who is or was associated with or employed by the Adams Campaigns to provide benefits, whether lawfully or unlawfully, to [REDACTED] or his employees or associates in exchange for campaign contributions.

C. Evidence relating to payments to employees, officers, and associates of [REDACTED] to facilitate those employees, officers, and associates making campaign contributions to the Adams Campaigns.

D. Evidence relating to the source of funds for payment or reimbursement of employees, officers, and associates of [REDACTED] or other persons serving as conduits for campaign contributions to the Adams Campaigns.

E. Evidence of individuals or entities who donated to the Adams Campaigns before or after receiving transfers of funds similar to the amount of the donation.

F. Evidence regarding the identity of any persons or entities involved, wittingly or unwittingly, in donations to the Adams Campaign in which the named donor is not the true source of the donated funds (“straw donations”).

G. Evidence of the relationship between and among [REDACTED] the Government of Uzbekistan, any persons involved in straw donations to the Adams Campaigns or any person who is or was associated with or employed by the Adams Campaigns, including all communications with or about, contact information for, and meetings and appointments with co-conspirators.

H. Evidence of an intent to exchange benefits between [REDACTED] or his employees or associates, and the Adams Campaigns or any person who is or was associated with or employed by the Adams Campaigns.

I. Evidence regarding any requests by the Adams Campaigns for matching funds based on donations from [REDACTED] personnel or persons associated with [REDACTED] or any other straw donors, including any discussions of matching funds.

J. Evidence regarding efforts to move funds into the United States and among accounts in order to disguise the true source and character of the funds.

K. Passwords or other information needed to access the user’s online accounts, including encrypted data stored in the Seized Devices.

L. Evidence sufficient to establish the owners and users of the Seized Devices at times relevant to the Subject Offenses.

M. Evidence of the geographic location of users, computers, or devices involved in the commission of the Subject Offenses at times relevant to the Subject Offenses.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the SUBJECT PREMISES also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section A of this Attachment above, including, but not limited to, desktop and laptop computers, cellphones, and tablets (including iPads). In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

Included within the items to be seized from the SUBJECT PREMISES are:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Accessing ESI

During execution of the search of the SUBJECT PREMISES authorized herein, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of [REDACTED] to any device found at the premises reasonably believed by law enforcement to be used by [REDACTED] (2) hold any such device in front of [REDACTED]'s face and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

D. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

UNITED STATES DISTRICT COURT

for the
Eastern District of New YorkIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)IN THE MATTER OF SEARCH OF PREMISES KNOWN AS [REDACTED]
[REDACTED] BROOKLYN, NEW YORK 11234, AND ANY AND ALL COMPUTERS,
CELLULAR TELEPHONES AND ELECTRONIC DEVICES CONTAINED
THEREIN

Case No. 24-MC-2339

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Eastern District of New York
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before June 26, 2024 (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of .Date and time issued: June 12, 2024 6:22 pm
Judge's signatureCity and state: Brooklyn, New YorkHon. Peggy Kuo U.S.M.J.
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:

24-MC-2339

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

Premises to be Searched—Subject Premises

The premises to be searched (the “SUBJECT PREMISES”) are described as follows, and include all locked and closed containers found therein:

The SUBJECT PREMISES is a detached single-family home located at [REDACTED] [REDACTED] Brooklyn, New York 11234. The SUBJECT PREMISES is accessed by a door up a short flight of stairs from the driveway and sidewalk, with the number “[REDACTED]” inscribed on an archway approaching the doors. A photograph of the SUBJECT PREMISES, as well as and a close-up of the archway before the door, is included below.





ATTACHMENT B

Items to Be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the SUBJECT PREMISES consist of the following evidence, fruits, and instrumentalities of violations (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds and conspiracy to steal federal funds, federal program bribery, and conspiracy to commit the same), (ii) 18 U.S.C. §§ 1343 and 1349 (wire fraud and attempt and conspiracy to commit wire fraud), (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same), and (iv) 18 U.S.C. § 1956 (money laundering and conspiracy to commit money laundering) (collectively, the “SUBJECT OFFENSES”), described as follows:

1. Evidence concerning occupancy or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys.

2. Electronic devices, including cellphones, laptops, and tablets, owned or used by [REDACTED] (hereinafter, the “Seized Devices”).

3. Evidence regarding the identity of the owner or user of the Seized Devices at times relevant to the Subject Offenses.

The Seized Devices may be searched for the following evidence, fruits, and instrumentalities of the Subject Offenses:

A. Evidence of knowledge or understanding of, or intent to violate, laws and regulations governing the conduct of the Adams Campaigns on the part of [REDACTED] and his employees or associates, or the Adams Campaigns.

B. Evidence relating to coordination between [REDACTED] and the Adams Campaigns concerning political contributions to the Adams Campaigns, including, but not limited to, evidence of motive and intent for [REDACTED] or his employees or associates to provide or facilitate campaign contributions to the Adams Campaigns, and evidence of motive and intent by any person who is or was associated with or employed by the Adams Campaigns to provide benefits, whether lawfully or unlawfully, to [REDACTED] or his employees or associates in exchange for campaign contributions.

C. Evidence relating to payments to employees, officers, and associates of [REDACTED] to facilitate those employees, officers, and associates making campaign contributions to the Adams Campaigns.

D. Evidence relating to the source of funds for payment or reimbursement of employees, officers, and associates of [REDACTED] or other persons serving as conduits for campaign contributions to the Adams Campaigns.

E. Evidence of individuals or entities who donated to the Adams Campaigns before or after receiving transfers of funds similar to the amount of the donation.

F. Evidence regarding the identity of any persons or entities involved, wittingly or unwittingly, in donations to the Adams Campaign in which the named donor is not the true source of the donated funds (“straw donations”).

G. Evidence of the relationship between and among [REDACTED] the Government of Uzbekistan, any persons involved in straw donations to the Adams Campaigns or any person who is or was associated with or employed by the Adams Campaigns, including all communications with or about, contact information for, and meetings and appointments with co-conspirators.

H. Evidence of an intent to exchange benefits between [REDACTED] or his employees or associates, and the Adams Campaigns or any person who is or was associated with or employed by the Adams Campaigns.

I. Evidence regarding any requests by the Adams Campaigns for matching funds based on donations from [REDACTED] personnel or persons associated with [REDACTED] or any other straw donors, including any discussions of matching funds.

J. Evidence regarding efforts to move funds into the United States and among accounts in order to disguise the true source and character of the funds.

K. Passwords or other information needed to access the user’s online accounts, including encrypted data stored in the Seized Devices.

L. Evidence sufficient to establish the owners and users of the Seized Devices at times relevant to the Subject Offenses.

M. Evidence of the geographic location of users, computers, or devices involved in the commission of the Subject Offenses at times relevant to the Subject Offenses.

B. Search and Seizure of Electronically Stored Information

The items to be seized from the SUBJECT PREMISES also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section A of this Attachment above, including, but not limited to, desktop and laptop computers, cellphones, and tablets (including iPads). In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

Included within the items to be seized from the SUBJECT PREMISES are:

1. Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.
2. Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.
3. Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

C. Accessing ESI

During execution of the search of the SUBJECT PREMISES authorized herein, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of [REDACTED] to any device found at the premises reasonably believed by law enforcement to be used by [REDACTED] (2) hold any such device in front of [REDACTED] face and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

D. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

EXHIBIT 1

[24 MAG 1398]

EXHIBIT 2

[24 MAG 2164]